IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF PENNSYLVANIA

APRIL COBB, *on behalf of herself and all others similarly situated*, Plaintiff, vs. TESLA, INC., doing business as TESLA MOTORS, INC. Defendant.	CIVIL ACTION NO.

CLASS ACTION COMPLAINT

I. INTRODUCTION

1. On May 10, 2023, Defendant Tesla, Inc. d/b/a Tesla Motors, Inc. (hereinafter "Tesla") had its data breached by unauthorized hackers (the "Data Breach"), who stole the highly sensitive personal identifying information ("PII") of Plaintiff and presumably thousands of former Tesla employees like her.

2. Companies such as Tesla that handle sensitive PII owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private financial matters.

3. The harm resulting from a data and privacy breach manifests in a number of ways, including, but not limited to: (a) identity theft and financial fraud and time spent mitigating or preventing those issues; (b) exposure of a person's PII

through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives; and (c) lost or diminished value of a person's PII. Mitigating these risks—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take a number of additional prophylactic measures.

4. As a large, sophisticated corporation, Tesla knowingly collects and stores a litany of highly sensitive PII from its current and former employees. In turn, Tesla has a resulting duty to secure, maintain, protect, and safeguard the PII that it collects and stores against unauthorized access and disclosure through reasonable and adequate data security measures.

5. Tesla expressly recognizes its duty to securely maintain its employees' PII in confidence. Its "Tesla Talent Privacy Notice" states that "Tesla uses security measures to protect your personal data from loss, misuse and unauthorized access, disclosure, alteration and destruction. The security measures are implemented and maintained in accordance with legal, organizational, and technological developments."

6. Despite Tesla's duty to safeguard its employees' PII, the PII of Plaintiff and other Tesla employees and former employees was allowed to be accessed and exposed to an unauthorized third party during the Data Breach.

7. Based on the statements of Tesla to date, a variety of PII was implicated in the Data Breach, including but not limited to: names, Social Security Numbers, and birthdates.

8. As a direct and proximate result of Tesla's inadequate data security measures, and its breach of its duty to handle PII with reasonable care, the PII of Plaintiff and the Class Members have been accessed by hackers and exposed to an untold number of unauthorized individuals.

9. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, intrusion of their financial privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes. Additionally, Plaintiff and Class Members have also lost the value of their PII, for which there is an established marketplace value.

10. Plaintiff, on behalf of herself and the Class as defined herein, brings claims for negligence, breach of an implied contract, and breach of confidence, seeking actual and punitive damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

II. JURISDICTION

11. This Court has jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), codified in pertinent part at 28 U.S.C. § 1332(d).

12. Venue is proper in this District as the Defendant is registered to do business in Pennsylvania, and regularly conducts business in this District, including the Bethlehem, Northampton County, PA facility where the Plaintiff worked.

III. PARTIES

13. Plaintiff, April Cobb, is a consumer and natural person presently residing in Dallas, TX.

14. Plaintiff was an employee of Tesla and provided her personal information and PII to Tesla.

15. Plaintiff worked in Tesla's business location at 5210 Jaindl Blvd., Bethlehem, Northampton County, PA 18017 for the entire duration of her employment at Tesla.

16. Tesla notified Plaintiff of the Data Breach and the unauthorized access of her PII by sending her a "Notice of Data Incident" letter dated August 23, 2023.

17. Tesla, Inc. d/b/a Tesla Motors, Inc. ("Tesla") operates throughout the country, including in Pennsylvania and this District.

18. Tesla does substantial business in in this District, including but not limited to serving its existing customers by maintaining dozens of Superchargers among four stations located at:

a. 34 South 11th Street, Philadelphia, PA 19107;

b. 2501 Church Street, Philadelphia, PA 19124;

c. 420 North 20th Street, Philadelphia, PA 19130; and,

d. 2600 Penrose Avenue, Philadelphia, PA 19145.

19. Tesla, Inc. is registered as a Foreign Business Corporation with Pennsylvania's Department of State, with a registered address of CT Corporation System, 600 N. 2d St. #401, Harrisburg, PA.

IV. FACTS

Tesla Collected and Stored the PII of Plaintiff and Class Members

20. Due to the nature of its business, Tesla acquires, collects, and stores the PII of Plaintiff and the Class Members.

21. As a condition of providing employment to Plaintiff and Class Members, Tesla receives, creates, and handles PII, which include, *inter alia* employees' Social Security Numbers, dates of birth, addresses, phone numbers, and email addresses.

22. Plaintiff and Class Members are all employees or former employees who directly or indirectly entrusted Tesla with their sensitive and confidential PII and therefore reasonably expected that Tesla would safeguard their highly sensitive information and keep their PII confidential.

23. By obtaining, collecting, and storing the PII of Plaintiff and the Class Members, Tesla assumed equitable and legal duties to safeguard and keep confidential such highly sensitive information, to only use this information for employment and legitimate business purposes, and to only make authorized disclosures.

24. Indeed, Tesla expressly recognizes its duty to securely maintain its employees' PII in confidence. Its 2019 "Tesla Talent Privacy Notice" states that "Tesla uses security measures to protect your personal data from loss, misuse and unauthorized access, disclosure, alteration and destruction. The security measures are implemented and maintained in accordance with legal, organizational, and technological developments."

25. Despite these duties, Tesla failed to implement reasonable data security measures to protect Plaintiff's and Class Members' PII, and ultimately allowed nefarious hackers to breach the systems housing PII, compromising the PII of Plaintiff and the Class Members.

Tesla Knew the Risks and the Foreseeable Harm to Employees

26. At all relevant times, Tesla knew it was storing sensitive PII and that as a result, its systems would be attractive for cybercriminals.

27. Tesla also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, as well as intrusion into their highly private financial information.

28. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, and many others.

29. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as well as the "proliferation of

open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[1]

30. Numerous sources cite dark web pricing for stolen identity credentials. For example, in 2019, personal information could be sold at a price ranging from $40 to $200, and bank details had a price range of $50 to $200.[2] Other sources report that criminals can also purchase access to entire company data breaches from $999 to $4,995.[3]

31. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Tesla's employees and former employees especially vulnerable to identity theft, tax fraud, credit and bank fraud, and more.

32. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure

---

[1] Brian Krebs, *The Value of a Hacked Company*, KREBS ON SECURITY, July 14, 2016, http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[2] *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[3] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/. (last visited Aug. 30, 2023).

the harm resulting from data breaches cannot necessarily rule out all future harm."[4]

33. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as the name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

34. Based on the value of its employees' PII to cybercriminals, Tesla certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

The Data Breach

35. On or about August 23, 2023, Tesla announced to its employees and former employees in a "Notice of Data Incident" that it experienced a data breach.

36. According to Tesla, it was alerted by a "foreign media outlet" on May 10, 2023 that "it had obtained Tesla confidential information." Tesla said its

[4] U.S. GOVERNMENT ACCOUNTABILITY OFFICE, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION (June 2007), https://www.gao.gov/new.items/d07737.pdf.

investigation revealed that "two former Tesla employees misappropriated the information … and shared it with the media outlet."

37. Tesla says in the August 23, 2023 letter: "The personal information involved concerns data for certain current and former employees, including your name, certain contact information (such as address, phone number, and/or email address), date of birth, and social security number that Tesla maintains in the ordinary course of business in its capacity as an employer."

38. Despite being aware of the Data Breach in May 2023, Tesla failed to take any action to notify Plaintiff or other Class Members of the Data Breach until at least August 23, 2023.

39. Like Plaintiff, the Class Members received similar notices informing them that their PII was exposed in the Data Breach.

40. Upon information and belief, similar notices were sent to thousands of current and former Tesla employees across the country.

Defendant's Failed Response to the Breach

41. At least three months after Defendant claims to have discovered the Data Breach, Defendant began sending the Notice to persons whose PII Defendant confirmed was potentially compromised as a result of the Data Breach.

42. The Notice included, *inter alia,* basic details of the Data Breach, Defendant's recommended next steps, and Defendant's claims that it had learned of the "incident" on May 10, 2023.

43. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII with the intent of engaging in the misuse of the PII, including marketing and selling Plaintiff's and Class Members' PII.

44. Defendant had and continues to have obligations created by applicable federal and state law, reasonable industry standards, the common law, and its own assurances and representations to keep Plaintiff's and Class Members' PII confidential and to protect such PII from unauthorized access.

45. Plaintiff and Class Members were required to provide their PII to Defendant in order to be hired by Defendant. Defendant created, collected, and stored the PII of Plaintiff and the Class Members with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

46. Despite this, Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used, when Defendant learned about the breach, and what steps are being taken, if any, to secure their PII going forward. Plaintiff and Class Members are, thus, left to speculate as to where their PII ended up, who has used it, and for what potentially nefarious purposes, and are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities to prevent further breaches.

47. Unauthorized individuals can now easily access the PII and/or financial information of Plaintiff and Class Members.

48. Upon information and belief, Tesla failed to employ reasonable and adequate data security safeguards. The Data Breach occurred as a direct and proximate result of Tesla's failure to implement and follow basic security procedures in order to protect its employees' PII.

49. Defendant knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if Plaintiff's and Class Members' PII were stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude.

50. Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff and Class Members. Therefore, its failure to do so is intentional, willful, reckless, and/or grossly negligent.

51. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its systems were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII and/or financial information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach;

(iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

April Cobb's Experience

52. Plaintiff April Cobb is a victim of the Data Breach.

53. Plaintiff was an employee of Tesla, having formerly worked at the company's Bethlehem, PA location.

54. Plaintiff's personal identifying information was stored with Tesla as a result of her employment with Tesla.

55. As required in order to obtain employment from Tesla, Plaintiff provided the company with highly sensitive personal information, which Tesla then possessed and controlled.

56. As a result, Plaintiff's information was among the data accessed by an unauthorized third-party in the Data Breach.

57. At all times herein relevant, Plaintiff is and was a member of the Class.

58. Plaintiff received a letter from Defendant, dated August 23, 2023, stating that her PII may have been affected in the Data Breach (the "Notice").

59. Plaintiff was unaware of the Data Breach until receiving that letter.

60. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her

PII, in combination with her name, being placed in the hands of unauthorized third parties/criminals.

61. Plaintiff has a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ACTION ALLEGATIONS

62. Plaintiff brings this action on her own behalf and on behalf of a class pursuant to Rule 23 of the Federal Rules of Civil Procedure.

63. Plaintiff brings this action on behalf of the putative class defined as follows (the "Class"):

> All individuals within the United States of America whose PII was exposed to unauthorized third parties as a result of the data breach disclosed by Defendant in August 2023.

64. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

65. Plaintiff reserves the right to amend the above definitions or to propose subclasses in subsequent pleadings and motions for class certification.

66. The Class for whose benefit this action is brought is so numerous that joinder of all members is impracticable. It is believed, and therefore averred, that the class numbers in the thousands.

67. There are questions of law and fact common to the members of the Class that predominate over questions affecting only individuals, including but not limited to:

A. Whether Defendant had a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and/or safeguarding their PII;

B. Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

C. Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

D. Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

E. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

F. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

G. How and when Defendant actually learned of the Data Breach;

H. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiff and Class Members;

I. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

J. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members and/or by failing to timely notify Plaintiff and the Class Members of the same;

K. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendant's wrongful conduct;

L. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and,

M. Whether Plaintiff and the Class Members are entitled to damages.

68. A class action is superior to other available methods for the fair and efficient adjudication of this matter.

69. A class action will cause an orderly and expeditious administration of the claims of the Class and will foster economies of time, effort, and expense.

70. Plaintiff's claims are typical of the claims of the members of the Class.

71. The questions of law and/or fact common to the members of the Class predominate over any questions affecting only individual members.

72. Plaintiff does not have interests antagonistic to those of the Class.

73. The Class, of which Plaintiff is a member, is readily identifiable through Defendant's own records and the mailing of the "Notice of Data Incident."

74. Plaintiff will fairly and adequately protect the interests of the Class and have retained competent counsel experienced in the prosecution of consumer class action litigation. Class Counsel have investigated and identified potential claims in the action; have a great deal of experience in handling consumer class actions, other complex litigation, and claims of the type asserted in this action.

75. The prosecution of separate actions by individual members of the Class (1) would run the risk of inconsistent or varying adjudications that would establish

incompatible standards of conduct for the Defendant in this action or (2) would create the risk that adjudications with respect to individual members of the class would as a practical matter be dispositive of the interests of the other members not parties to the adjudications or substantially impair or impede their ability to protect their interests. Prosecution as a class action will eliminate the possibility of repetitious litigation.

76. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety.

77. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiff.

78. Unless a Class-wide injunction is issued, Defendant may continue failing to properly secure the PII and/or financial information of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

79. Plaintiff does not anticipate any difficulty in the management of this class litigation.

VI. CLAIMS FOR RELIEF

COUNT I – NEGLIGENCE

80. Plaintiff, on behalf of herself and the Class, reasserts and incorporates herein the allegations contained in the preceding and following paragraphs.

81. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of care, *inter alia,* to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PII of Plaintiff and Class Members in its computer systems and on its networks.

82. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession;

b. to protect Plaintiff's and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and to promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

83. Defendant knew that the PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care

not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

84. Defendant knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security.

85. Defendant knew about numerous, well-publicized data breaches.

86. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

87. Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII that Plaintiff and Class Members had entrusted to it.

88. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PII.

89. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the PII contained therein.

90. Plaintiff's and Class Members' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions.

91. Moreover, only Defendant had the ability to protect its systems and the PII that is stored on them from attack. Thus, Defendant had a special relationship with Plaintiff and Class Members.

92. Defendant also had independent duties under laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PII and promptly notify them about the Data Breach.

93. Defendant breached its general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members;
b. by failing to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed;
c. by failing to adequately protect and safeguard the PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII;
d. by failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class Members, misuse the PII and intentionally disclose it to others without consent;
e. by failing to adequately train its employees not to store PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PII;

g. by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and,

h. by failing to encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

94. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

95. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages.

96. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII to Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PII.

97. Defendant breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting at least three months after learning of the Data Breach to notify Plaintiff and Class Members and then by failing and continuing to fail to provide Plaintiff and Class Members sufficient information regarding the breach.

98. To date, Defendant has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and Class Members.

99. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII.

100. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

101. Plaintiff's and Class Members' PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

102. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

103. The damages Plaintiff and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

104. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-

of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

105. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II – BREACH OF IMPLIED CONTRACT

106. Plaintiff, on behalf of herself and the Class, reasserts and incorporates herein the allegations contained in the preceding and following paragraphs.

107. Through its course of conduct, Defendant, Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

108. Defendant required Plaintiff and Class Members to provide and entrust their PII as a condition of employment.

109. Defendant solicited and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices.

110. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

111. As a condition of being direct employees of Defendant, Plaintiff and Class Members provided and entrusted their PII to Defendant.

112. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

113. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Defendant, in exchange for, amongst other things, the protection of their PII.

114. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

115. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

116. As a direct and proximate result of Defendant's breach, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

117. As a direct and proximate result of Defendant's breach, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury

and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

118. Additionally, as a direct and proximate result of Defendant's breach, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT III – BREACH OF CONFIDENCE

119. Plaintiff, on behalf of herself and the Class, reasserts and incorporates herein the allegations contained in the preceding and following paragraphs.

120. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Tesla and that was ultimately accessed or compromised in the Data Breach.

121. As employer entrusted with sensitive information, Tesla has a special relationship with its employees and former employees, like Plaintiff and the Class Members.

122. Because of that special relationship, Tesla was provided with and stored private and valuable PII related to Plaintiff and the Class, which it was required to maintain in confidence.

123. Plaintiff and the Class provided Tesla with their personal and confidential PII under both the express and/or implied agreement of Tesla to limit the use and disclosure of such PII.

124. Tesla owed a duty to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

125. Tesla had an obligation to maintain the confidentiality of Plaintiff's and Class Members' PII.

126. Plaintiff and Class Members have a privacy interest in their PII, and Tesla had a duty not to disclose confidential information and records concerning its employees and former employees.

127. As a result of the parties' relationship, Tesla had possession and knowledge of confidential PII of Plaintiff and Class Members.

128. Plaintiff's and Class Members' PII is not generally known to the public and is confidential by nature.

129. Plaintiff and Class Members did not consent to nor authorize Tesla to release or disclose their PII to a criminal actor.

130. Tesla breached the duties of confidence it owed to Plaintiff and Class Members when Plaintiff's and the Class Members's PII was disclosed to criminal hackers.

131. Tesla breached its duties of confidence by failing to safeguard Plaintiff's and Class Members' PII, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of employee information

that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its members; (h) storing PII in a vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class Members' PII to a criminal third party.

132. But for Tesla's wrongful breach of its duty of confidences owed to Plaintiff and Class Members, their privacy, confidences, and PII would not have been compromised.

133. As a direct and proximate result of Tesla's breach of Plaintiff's and Class Members' confidences, Plaintiff and Class Members have suffered injuries, including:

a. Loss of their privacy and confidentiality in their PII;

b. Theft of their PII;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Tesla with the mutual understanding that Tesla would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Tesla's possession and is subject to further breaches so long as Tesla fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

j. Mental anguish accompanying the loss of confidences and disclosure of their confidential and private PII.

134. As a direct and proximate result of Tesla's breach of its duty of confidences, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and each member of the proposed Class, respectfully requests that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify the proposed class, including the appointment Plaintiff Cobb as Class Representative and of Plaintiff's counsel as Class Counsel;
2. For an award of damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering them to cease from unlawful activities;
4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;
5. For injunctive relief other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:
    a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
    b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
    c. requiring Defendant to delete and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. requiring Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems periodically;

f. prohibiting Defendant from maintaining Plaintiff's and Class Members' PII on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII;

k. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested, and updated; and

l. requiring Defendant to meaningfully educate all Class Members about the threats they face due to the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded;

7. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law; and

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

VIII. JURY DEMAND

Plaintiffs demand trial by jury as to all claims and defenses.

Dated: September 20, 2023

s/Andrew M. Milz
FLITTER MILZ, P.C.
Cary L. Flitter
Andrew M. Milz
Jody Thomas López-Jacobs
450 N. Narberth Ave., Suite 101
Narberth, PA 19072
Tel.: (610) 822-0781
Fax.: (833) 775-3450
amilz@consumerslaw.com
jlopez-jacobs@consumerslaw.com

FRANCIS MAILMAN SOUMILAS, P.C.
James A. Francis
Jordan Sartell
1600 Market Street, Suite 2510
Philadelphia, PA 19103
Tel: (215) 735-8600
Fax: (215) 940-8000
jfrancis@consumerlawfirm.com
jsartell@consumerlawfirm.com

Attorneys for Plaintiff and the Class